US Army Cyber Command/2nd Army

Training Soldiers to Prevent/Shape/Win in Cyberspace

24 October 2012

		Form Approved OMB No. 0704-0188
Report Documentation Page	

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **24 OCT 2012**	2. REPORT TYPE	3. DATES COVERED **00-00-2012 to 00-00-2012**
4. TITLE AND SUBTITLE **Training Soldiers to Prevent/Shape/Win in Cyberspace**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Cyber Command/2nd Army,Fort Belvoir,VA,22060**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 2012 Association United States Army (AUSA) Annual Meeting Oct 22-24, 2012

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Warfighting Domains

LAND

SEA

AIR

SPACE

CYBER

UNKNOWN

The Operational Environment

" In war, the objective of a commander is to accomplish victory at the smallest possible cost and loss, and the means whereby he attains his objective in the field is by developing mobility through protected offensive power. He strives to attain freedom of movement and action through combining a variety of arms." – COL J.F.C Fuller, *Infantry Journal*, May 1927.

Challenges

- **68,000 hacker tools**
  - **Android malware Up 500% in 1 year**
- **McAfee malware repository at 75 Mil**
  - **DoD counters 50K emails a month**
- **80% of malware is hosted within U.S.**
- **Botnets send 89.5 Billion emails daily**
- **In 2011**
  - **Attacks on critical infrastructure up from 9 (2009) to 168 (2011)**
  - **Attacks rose by 44%**
  - **Malware Up 60%**
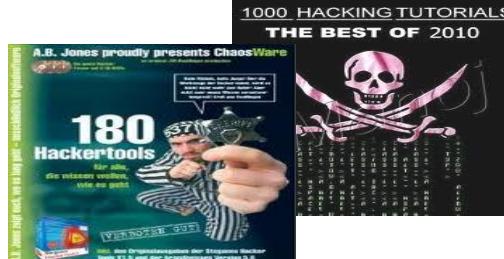
- **10 Billion Mobile Devices (Worldwide)**
  - **More time on apps than internet**
  - **50 Million have cellphone but no electricity**
  - **500,000 apps for IPHONE**
  - **280,000 apps for Android**
  - **In 2011, 107 Trillion emails sent**
- **165 Million US Cell Phone users**
- **90 Million check email daily using phone**
- **461 Million Mobile devices sold in 2011**

- **Worldwide internet users**
  - **In 2000, 360 Million users**
  - **1st Qtr 2012, 2.3 Billion (38% of world pop.)**
  - **3.2 Billion email accounts worldwide**
  - **In 2011, 107 Trillion emails sent**
- **US Hosts 431K (43%) of worlds top 1 Million websites**
- **FaceBook reached 1 Billion users Aug 12**

U.S. ARMY CYBER COMMAND / U.S. 2ND ARMY

Cyber Defense

PREVENT

SHAPE

S Strategic

O Operational

T Tactical

- **Trained and ready cyber forces**

- **Capacity/Capability**
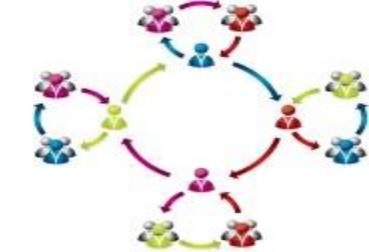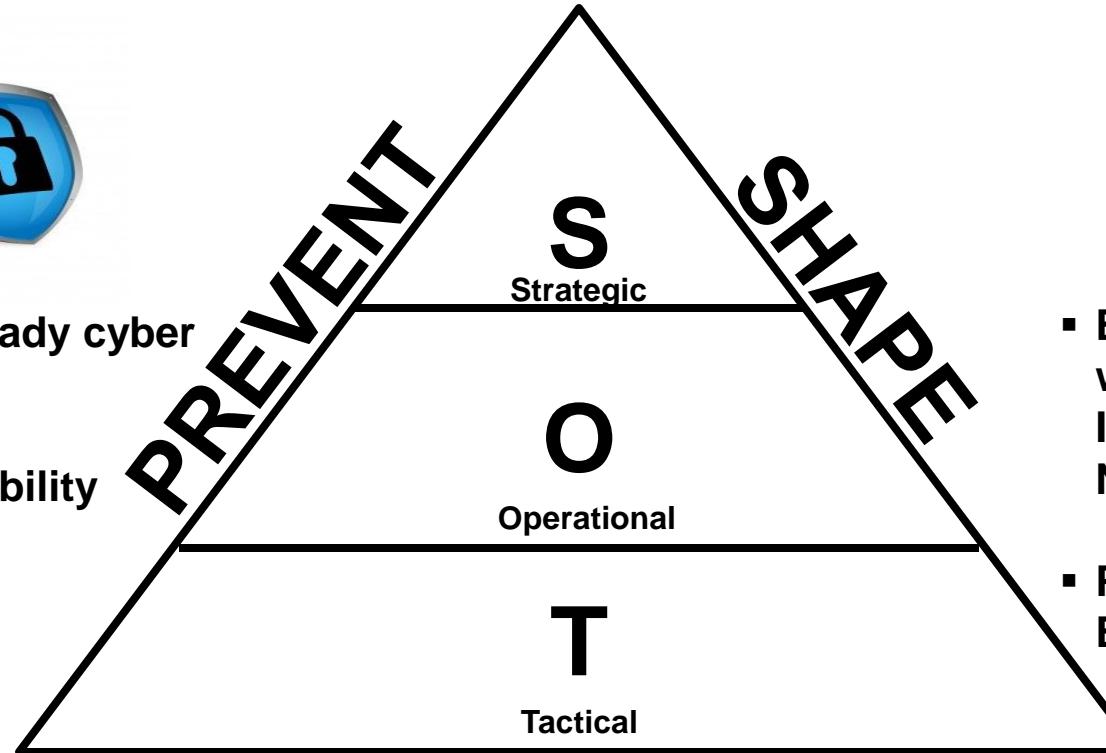
- **Build partner capacity with Government, Industry, and Allied Nations**

- **Prepare the Environment**

Operating in Degraded Environments   **WIN!**   **Defending/Securing Critical Information**

U.S. ARMY CYBER COMMAND / U.S. 2ND ARMY

Centers of Excellence

Inextricably Linked & Mutually Supporting

35 Q
Cryptologic Network Specialist

CORE FUNCTIONS

- **Collect & Analyze Data**
- **Detect, Track, Report**
- **& Exploit Threats**
- **Provide Trends, Indications, & Warnings**
- **Conduct Integrated Cyber Operations**
- **& Cyber BDA**

25 D
Cyber Network Defender

CORE FUNCTIONS

- **Plan and Engineer the Network**
- **Install and Operate the Network**
- **Command and Control the Network**
- **Maintain the Network**
- **Conduct Cyber Defense**
- **Provide Network Defense**
- **Maintain CyberSA**

What Leaders need to know

1. Embrace cyberspace as **Contested Domain**
2. **Know the Threat**…. Its not random
3. Treat the Network as a **Weapon System**
4. Identify and **Protect Key Cyber Terrain**
5. Strong **2-3-6** Integration- Required to Enable Mission Command
6. **Enforce Compliance** with Basic Standards and Discipline…. Information Assurance is not a given – Remediation is Expensive
7. This is **Leader's Business**
8. Conduct **Training and Leader Development**
9. Support IT Reform – Necessary but not Sufficient
10. Make **People the Centerpiece**, not Technology

Protect the Force….Maintain Our Freedom to Operate

US Army Cyber Command/2nd Army

QUESTIONS